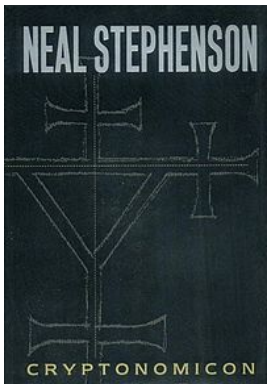
Cryptonomicon Avon, 1999, ISBN 0-380-97346-4, 918 pp; Luitingh-Sijthoff, 2001, ISBN 90-245-3718-5, 1085 pp; Livre de Poche, (3 volumes) 2001, ISBN 978-2253072362, 541 pp.; 2002, ISBN 978-2253072447, 540 pp.; 2003 ISBN 978-2253072553, 576 pp. by *Neal Stephenson*.

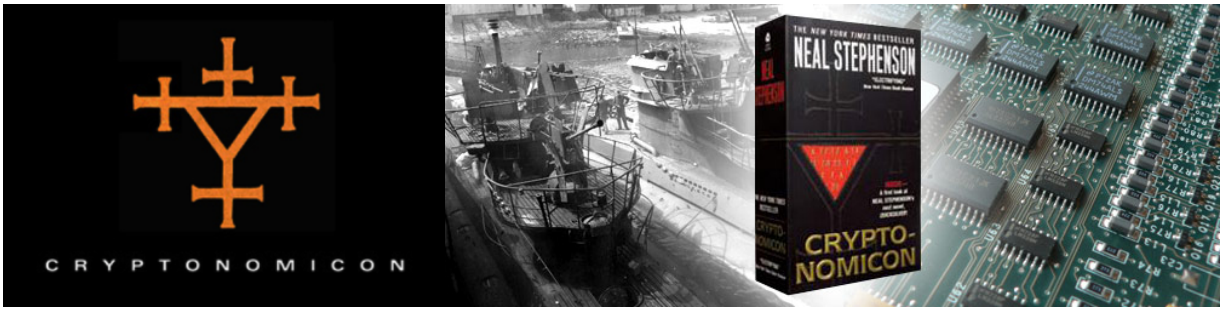


Neal Stephenson

Those we read my reviews here will know that Neal Stephenson is one of my favorite authors. His *Cryptonomicon* is actually a classic from 1999. However, since the Turing year in 2012 and the film *The imitation game* from 2014, cryptography became again a hip topic. So this might be as good an occasion as any to pick up the book again. Although Stephenson is not a mathematician, cryptography seems to be one of his hobbies. It appears in this book and in at least two of his subsequent books: In *Quicksilver*[1] and in *The diamond age*[2] where he describes a Turing machine. We still find some mathematics in *Anathem*[3] but not cryptography as such.

You can imagine that he can put a lot of characters, adventures, plots, violence and sex in about 1000 pages, but also a lot of mathematics and the latter is somewhat unusual in a novel. Not for Neal Stephenson though. It is *the* techno-thriller *par excellence* that circulated as "the ultimate geek novel" a number of years ago.

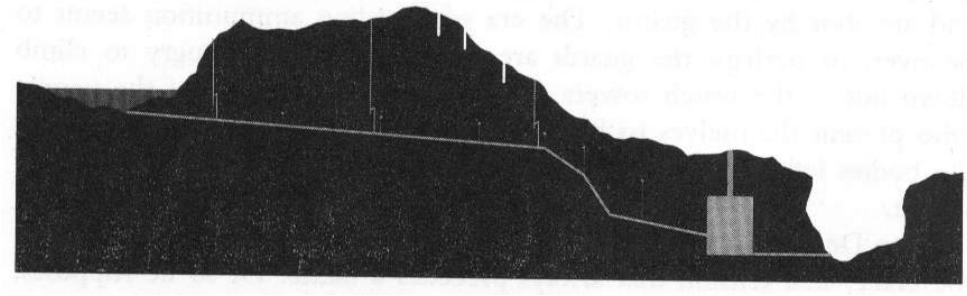
I will not explain all fictional and historical characters as they are entangled in the complex plot. It is just too complicated and it might take the tension away when you want to read it. So only in general terms: Part of the events play during and shortly after World War II when the code breakers (among them Alan Turing) at Bletchley Park near London succeeded in decrypting the messages that were encoded by the German Enigma machines. This was extremely important to know the maneuvers of the German submarines, and other strategic plans of the Axis Allience. However, it was equally important to prevent that the Germans would detect that the code had been cracked, because then they would immediately change their strategy and all the code breaking effort would be lost. So there was a special unit whose main task was to set up a smoke screen for the Germans, so that the successes of the Allied Forces could be explained by pure coincidence not pointing to an interception of coded messages.



In the novel Lawrence Pritchard Waterhouse is an American code breaker who is involved in this operation. The fighting machine Bobby Shaftoe is an American marine who has to execute some of these jobs behind enemy lines. Shaftoe has an earlier Japanese friend Goto Dengo, who at the time of the war is the enemy. He is building some tunnels and a vault in the Philippines

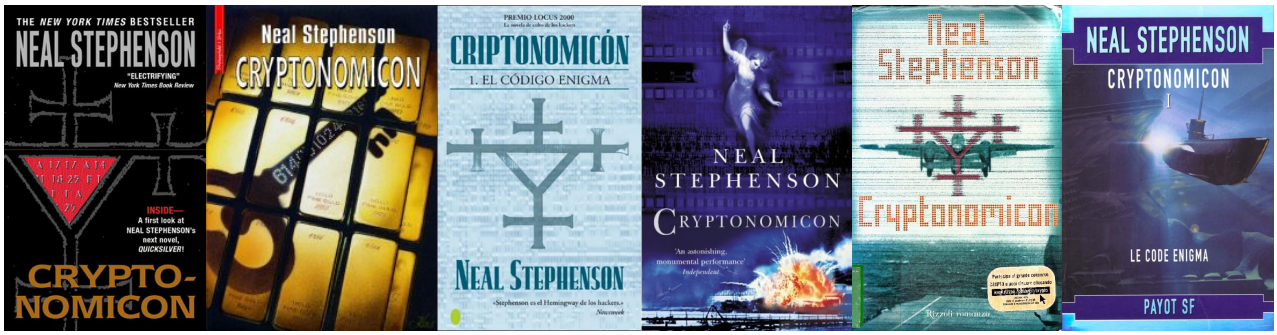
[1] This Newsletter, issue 54, September 2005.
[2] This Newsletter, issue 89, September 2012.
[3] This Newsletter, issue 86, January 2012.

where a massive stock of looted gold has to be buried. All workers are supposed to die when this underground system is detonated, but he escapes together with some Chinese slave Mr. Wing.



Construction of crypt by Goto Dengo to store the gold

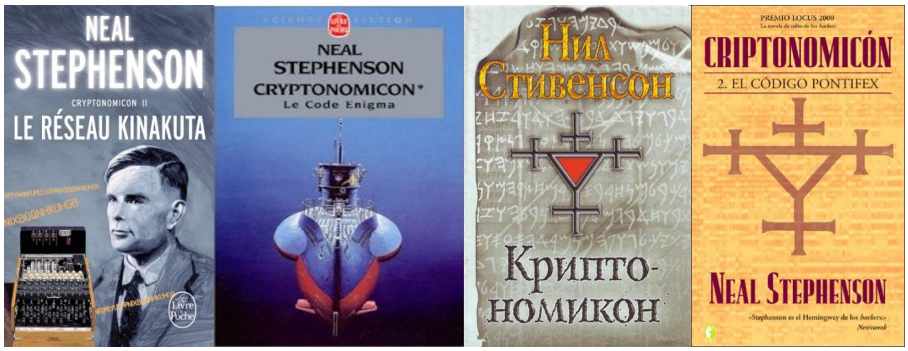
Another part of the story takes place late 1990's where several characters reappear at a later stage of their livesand others are descendants from the people in the first period. Here Randy Lawrence Waterhouse, grandson of Lawrence Pritchard, is a programmer trying to sell software in the Philippines for cheap instant communication. His friend Avi Halaby is CEO of an IT company called *Epiphyte* that is trying to set up a *data haven* nearby. So they become interested in the underwater fiber optic communication cables being installed by a company run by the son of Goto Dengo, and they get help from divers who happen to be the son and granddaughter of Bobby Shaftoe. Anyway, because of legal problems, the objective changes into treasure hunting for gold by several competitors, some who knew, and some who detected it by finally breaking a Japanese code *Arethusa*.



The title Cryptonomicon refers to some fictional *Kabbalah* of cryptography that was started by John Wilkins (1614-1672), one of the founders of the *Royal Society*, as one can read in *Quicksilver*. It is continuously updated by selected people and Lawrence Waterhouse is one of them. This Wilkins is an historical figure, and Stephenson mixes several of them in this novel. There are Turing, von Neumann, and Einstein, Douglas MacArthur, Ronald Reagan, and Isoroku Yamamoto and he embeds historical events as well. For example the Americans used Navajo talkers during the war because that was a language spoken by few and hence could not be understood by the enemy. Stephenson creates a fictional archipelago Qwghlm (pronounced Taghum) of two islands inspired by the Outer Hebrides where a language is spoken lacking vocals. It is a British equivalent of the American Navajo language. This is a rather funny episode. Mary cCmndhd (pronounced "Skuhmithid" and anglicized as "Smith") is a Qwghlmian character appearing later in the novel. Qwghlm is further elaborated in *Quicksilver*.

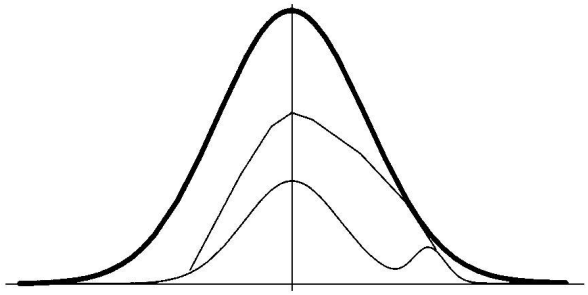
But let me move to the mathematics. Already in the first chapter we read about Turing and Lawrence Waterhouse discussing the evaluation of the zeta function in Princeton, later joined by Rudy Hacklheber, a (fictional) German cryptographer. They discuss Leibniz's symbols, Riemann, Euler, Russell and the *Principia Mathematica*, Gödel, a series expansion for π, and of course some elements of cryptography. Not exactly the start of an ordinary novel. The reader is introduced to elements of cryptography and how they could be decoded by detecting patterns in the code. It was very important to capture some of the Enigma machines from German U-boats, which has actually happened. Once the system is known, then it was important to find the key. In

Waterhouse's mind this cryptographic system the key is compared with a register to be chosen when playing an organ.



The unit that has to generate the smoke curtain for the Germans was originally called unit 2701, but Waterhouse objects because it is the product of two symmetric primes: 73 and 37. That would be too obviously suspicious for German cryptographers like Rudy, and hence the unit is renamed as 2702. When later in a grounded U-553, a safe has to be opened, the combination alternates left-right the numbers 23 - 37 - 7 - 31 - 13, all primes.

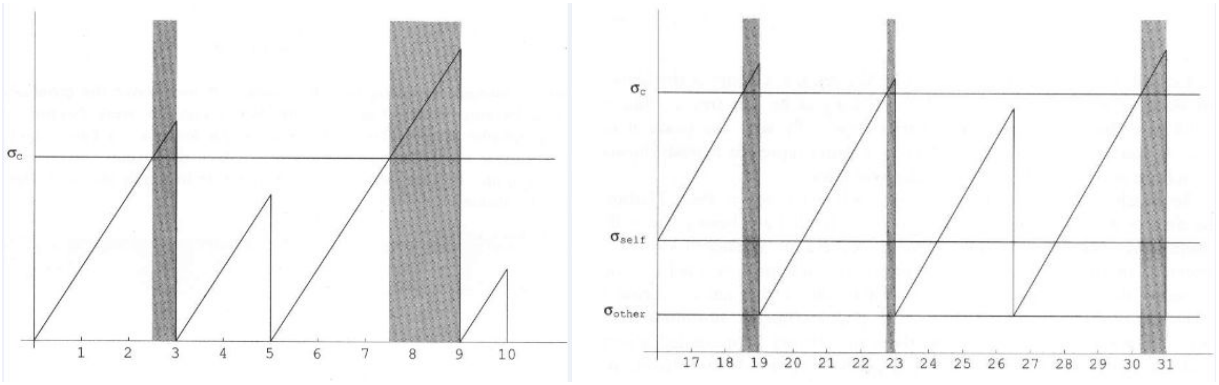
Waterhouse trying to decode the message from the safe consults Turing. Turing had returned from Princeton, now studying radio tubes, a new American technology. The code seems to be based on a one-time key generated by a very large (pseudo) random number that should be generated by some algorithm (could this involve the evaluation of the zeta function?) initiated by a relatively simple key (turns out later to be the date).



Cloaking the deviating Gauss shape

Some women working at Bletchley park should be larger than average because they had to reset highly placed switches at the *Bombe* machines that were computing the keys. This entails a discussion of Gaussian distribution of the length of female employees, which would show a side peak, and hence alert German intelligence agents. What would be a proper startegy to hide the side peak?

Modulo calculus is needed to avoid too frequent repetition in a generated sequence for the code. This is explained with a bicycle (Turing loved cycling) whose chain has a weak link that would break when coinciding with a tooth of the rear sprocket. When the number of links in the chain and the number of teeth in the sprocket have a small common multiple, the chain will break more frequently.



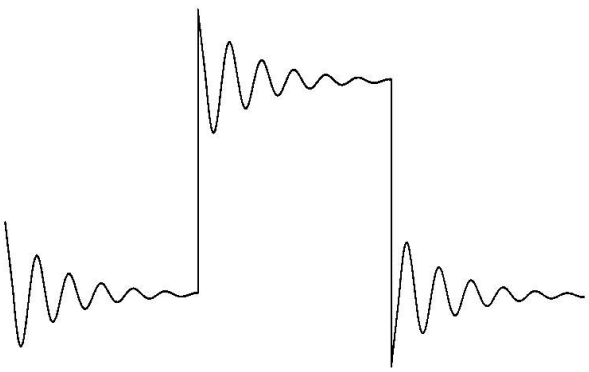
Waterhouse's performance graph

Another fun mathematical model, complete with graphs and formulas is worked out for how

Waterhouse is functioning in his code breaking job. He can only do creative thinking and hence be productive when he has satisfied his sex drift. So when his last ejaculation was too long ago, his horniness passes some threshold and he becomes unproductive. A new release can drop it to some lower level. A visit to a whorehouse brings this to a lower level than a 'Manual Override'. This gives some sawtooth function showing in which periods he is productive and when he is not. However, here Stephenson's formula is blatantly wrong. As the horniness σ approached the critical threshold σ_c, his clarity of mind C_m decreases from 1 to 0, and the number $N_{\rm dec}$ of decryptions decreases exponentially. The function $N_{\rm dec}(C_m)$ has a vertical asymptote near $C_m = 1$ and is practically zero near $C_m = 0$. Hence, writes Stephenson, $C_m \propto \lim_{n\to\infty} \frac{1}{(\sigma-\sigma_c)^n}$, which is not really what is intended here.

A knapsack-like problem has to be solved when dividing a legacy. The problem is to distribute n objects among m persons, each getting one of the shares $(S_1, \ldots, S_m)$ and the idea is that each subset has about the same value. However each person assigns a vector of values to the n objects. Some uncle Red, head of the department of mathematics has to solve this. He takes people outside and they can place objects in an (x, y) frame with x representing emotional value and y financial value.

Near the end a coding algorithm is used based on card shuffling of a pack of 52 cards and two distinct jokers. It is an output feedback mode stream cipher based on modulo calculus. The 52 is important because it is twice 26 the number of letters in the alphabet. The method is invented by Bruce Schneider and fully described in an appendix, but it can also be found on his website `www.schneier.com/solitaire.html`.



Another graph from the book
Transition phenomena described by Turing

There are many other geeky references, like the computers running a Finux operating system, clearly referring to the existing Unix or Linux developed the Fin Linus Torvalds. There is an actual perl script, (internet) security, phreasing, and an analysis of Greek mythology in the context of WW II. Even after some 1K pages, it is disappointing that you reached the end. But fortunately, he has other books too, and Stephenson is still very productive.

A. Bultheel